Cont. US 6,591,291

Japanese Patent Laid-open Publication No. HEI 11-161574 A

Publication date: Jun. 18, 1999

Applicant: LUCENT TECHNOL INC

Title: SYSTEM AND METHOD FOR PROVIDING EMAIL ANONYMOUS REMAIL AND FILTERING

(57) [Abstract]

[Object] To provide an anonymous remailer that can automatically filter emails and messages.

[Solution] This system includes an alias transmission source address creating unit that uses a destination address to create an alias transmission source address. This system also includes an alias transmission source address replacing unit that replaces an actual transmission source address with an alias transmission source address. Thus, an actual transmission source address can be deleted from an email and message, thereby making a transmitter who exists at the actual transmission source address anonymous. A reply email is transferred, and the reply email is filtered based on the alias transmission source address.

[0033] At step 350, a compressed actual transmission source address (with additional empty bytes) is encrypted according to, for example, a data encryption standard

(DES) that uses a unique extended secret key for a destination address as an encryption key. Security is increased by using a great number of DES paths. The type of encryption applied is not important. Encryption need not accord to DES, nor need it be asymmetrical. The present invention does not actually require any kind of encryption.

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号

特開平11－161574

(43)公開日　平成11年(1999)６月18日

| (51)Int.Cl.[6] | | 識別記号 | FI | |
|---|---|---|---|---|
| Ｇ０６Ｆ | 13/00 | ３５１ | Ｇ０６Ｆ　13/00 | ３５１Ｇ |
| Ｈ０４Ｌ | 12/54 | | Ｈ０４Ｌ　11/20 | １０１Ｂ |
| | 12/58 | | | |

審査請求　未請求　請求項の数41　ＯＬ　（全 10 頁）

(21)出願番号　特願平10－239336

(22)出願日　平成10年(1998)８月26日

(31)優先権主張番号　６０／０５７１３２

(32)優先日　1997年８月28日

(33)優先権主張国　米国（ＵＳ）

(31)優先権主張番号　０９／０４１２０９

(32)優先日　1998年３月12日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　596092698
ルーセント　テクノロジーズ　インコーポレーテッド
アメリカ合衆国．07974－0636　ニュージャーシィ，マレイ　ヒル，マウンテン　アヴェニュー　600

(72)発明者　エラン　ガバー
アメリカ合衆国　07901　ニュージャーシィ，サミット，ニュー　イングランド　アヴェニュー　15ビー

(74)代理人　弁理士　岡部　正夫　(外11名)

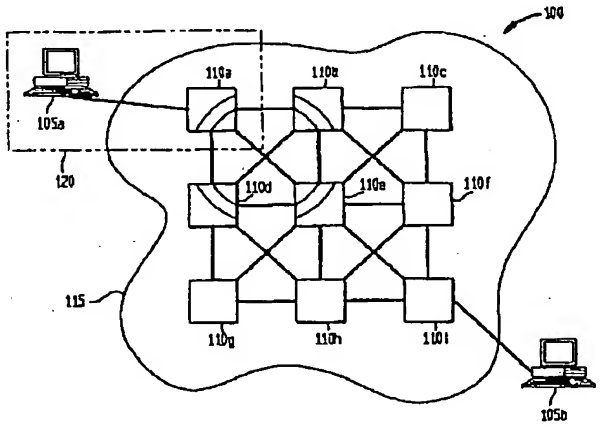
最終頁に続く

(54)【発明の名称】　電子メールの匿名リメールとフィルタリングを提供するシステムおよび方法

(57)【要約】

【課題】　電子メール・メッセージを自動的にフィルタリング可能な匿名リメーラを提供する。

【解決手段】　本システムには宛先アドレスを利用してエイリアス発信元アドレスを生成するエイリアス発信元アドレス生成器が含まれる。本システムにはさらに、実発信元アドレスをエイリアス発信元アドレスで置換するエイリアス発信元アドレス置換器が含まれる。これは電子メール・メッセージから実発信元アドレスを除去し、それによって実発信元アドレスに存在する送信者を匿名にする。返信電子メールを転送し、エイリアス発信元アドレスに基づいて返信電子メールをフィルタリングする。



1

【特許請求の範囲】

【請求項１】　実発信元アドレスと宛先アドレスを有する電子メール（ｅ－ｍａｉｌ）メッセージのエイリアス発信元アドレスを生成するシステムであって、
前記宛先アドレスを利用して前記エイリアス発信元アドレスを生成するエイリアス発信元アドレス生成器と、
前記実発信元アドレスを前記エイリアス発信元アドレスで置換するエイリアス発信元アドレス置換器であって、前記実発信元アドレスが前記電子メール・メッセージから除去されるエイリアス発信元アドレス置換器とを含むシステム。

【請求項２】　請求項１に記載のシステムにおいて、前記エイリアス発信元アドレス生成器が前記電子メール・メッセージの実発信元アドレスと前記宛先アドレスを利用して前記エイリアス発信元アドレスを生成するシステム。

【請求項３】　請求項２に記載のシステムにおいて、前記エイリアス発信元アドレス生成器が前記実発信元アドレスを圧縮して前記エイリアス発信元アドレスを生成するシステム。

【請求項４】　請求項１に記載のシステムにおいて、前記エイリアス発信元アドレス生成器が秘密鍵を利用して前記エイリアス発信元アドレスを生成するシステム。

【請求項５】　請求項１に記載のシステムにおいて、さらに、
前記エイリアス発信元アドレスから実発信元アドレスを生成する実発信元アドレス生成器と、
前記実発信元アドレス生成器に接続されるとともに、前記エイリアス発信元アドレスを前記実発信元アドレスで置換する実発信元アドレス置換器であって、前記実発信元アドレス生成器と置換器が協同して前記エイリアス発信元アドレス宛の電子メールが前記実発信元アドレスに転送されるようにすることができ、前記システムが電子メール転送器として機能する実発信元アドレス置換器とを含むシステム。

【請求項６】　請求項１に記載のシステムにおいて、前記エイリアス発信元アドレスが前記実発信元アドレスより長いシステム。

【請求項７】　請求項１に記載のシステムにおいて、さらに、前記エイリアス発信元アドレスに基づいて入り返信メールをフィルタリングできる電子メール・フィルタを含むシステム。

【請求項８】　実発信元アドレスと宛先アドレスを有する電子メール（ｅ－ｍａｉｌ）メッセージのエイリアス発信元アドレスを生成する方法であって、
前記宛先アドレスに基づいて前記エイリアス発信元アドレスを生成するステップと、
前記実発信元アドレスを前記エイリアス発信元アドレスで置換するステップであって、前記実発信元アドレスが前記電子メール・メッセージから除去されるステップとを含む方法。

2

【請求項９】　請求項８に記載の方法において、前記利用ステップが、前記エイリアス発信元アドレスを生成するために前記電子メール・メッセージの実発信元アドレスと前記宛先アドレスを利用するステップを含む方法。

【請求項１０】　請求項９に記載の方法において、前記利用ステップが、前記エイリアス発信元アドレスを生成するために、前記実発信元アドレスを圧縮するステップを含む方法。

【請求項１１】　請求項８に記載の方法において、前記利用ステップが、前記エイリアス発信元アドレスを生成するために秘密鍵を利用するステップを含む方法。

【請求項１２】　請求項８に記載の方法において、さらに、
前記エイリアス発信元アドレスから実発信元アドレスを生成するステップと、
前記エイリアス発信元アドレス宛の電子メールが前記実発信元アドレスに転送され、それによって前記電子メールが送られるように、前記エイリアス発信元アドレスを前記実発信元アドレスで置換するステップとを含む方法。

【請求項１３】　請求項８に記載の方法において、前記エイリアス発信元アドレスが前記実発信元アドレスより長い方法。

【請求項１４】　請求項８に記載の方法において、さらに、前記エイリアス発信元アドレスに基づいて入り返信メールをフィルタリングするステップを含む方法。

【請求項１５】　コンピュータ・ネットワークの複数のコンピュータ・システムの少なくとも１つに接続し、電子メール・メッセージのエイリアス発信元アドレスを生成し電子メール・メッセージをリメールするリメーラであって、
前記電子メール・メッセージの前記１つの宛先アドレスを利用して前記エイリアス発信元アドレスを生成するエイリアス発信元アドレス生成器と、
前記電子メール・メッセージの前記１つの前記実発信元アドレスを前記エイリアス発信元アドレスで置換するエイリアス発信元アドレス置換器であって、前記実発信元アドレスが前記電子メール・メッセージの前記１つから除去されるエイリアス発信元アドレス置換器と、
前記電子メール・メッセージの前記１つを前記宛先アドレスにリメールするデータ伝送回路とを含むリメーラ。

【請求項１６】　請求項１５に記載のリメーラにおいて、前記エイリアス発信元アドレス生成器が前記電子メール・メッセージの実発信元アドレスと前記宛先アドレスを利用して前記エイリアス発信元アドレスを生成するリメーラ。

【請求項１７】　請求項１６に記載のリメーラにおいて、前記エイリアス発信元アドレス生成器が前記実発信元アドレスを圧縮して前記エイリアス発信元アドレスを

生成するリメーラ。

【請求項１８】　請求項１５に記載のリメーラにおいて、前記エイリアス発信元アドレス生成器が秘密鍵を利用して前記エイリアス発信元アドレスを生成するリメーラ。

【請求項１９】　請求項１５に記載のリメーラにおいて、前記リメーラが、さらに、

前記エイリアス発信元アドレスから実発信元アドレスを生成する実発信元アドレス生成器と、

前記実発信元アドレス生成器に接続されるとともに、前記エイリアス発信元アドレスを前記実発信元アドレスで置換する実発信元アドレス置換器であって、前記実発信元アドレス生成器と置換器が協同して前記エイリアス発信元アドレス宛の電子メールが前記実発信元アドレスに転送されるようにすることができ、前記リメーラが電子メール転送器として機能する実発信元アドレス置換器とを含むリメーラ。

【請求項２０】　請求項１５に記載のリメーラにおいて、前記エイリアス発信元アドレスが前記実発信元アドレスより長いリメーラ。

【請求項２１】　請求項１５に記載のリメーラにおいて、前記リメーラが、さらに、前記エイリアス発信元アドレスに基づいて入り返信メールをフィルタリングできる電子メール・フィルタを含むリメーラ。

【請求項２２】　実発信元アドレスと宛先アドレスを有する電子メール（ｅ－ｍａｉｌ）メッセージのエイリアス発信元アドレスを生成するシステムであって、

前記宛先アドレスを利用して前記エイリアス発信元アドレスを生成するエイリアス発信元アドレス生成器と、

前記電子メール・メッセージに前記エイリアス発信元アドレスを配置するエイリアス発信元アドレス挿入器とを含むシステム。

【請求項２３】　請求項２２に記載のシステムにおいて、前記エイリアス発信元アドレス生成器が前記電子メール・メッセージの実発信元アドレスと前記宛先アドレスを利用して前記エイリアス発信元アドレスを生成するシステム。

【請求項２４】　請求項２３に記載のシステムにおいて、前記エイリアス発信元アドレス生成器が前記実発信元アドレスを圧縮して前記エイリアス発信元アドレスを生成するシステム。

【請求項２５】　請求項２２に記載のシステムにおいて、前記エイリアス発信元アドレス生成器が秘密鍵を利用して前記エイリアス発信元アドレスを生成するシステム。

【請求項２６】　請求項２２に記載のシステムにおいて、さらに、

前記エイリアス発信元アドレスから前記実発信元アドレスを生成する実発信元アドレス生成器と、

前記実発信元アドレス生成器に接続されるとともに、前記電子メール・メッセージに前記実発信元アドレスを配置する実発信元アドレス挿入器とを含むシステム。



【請求項２７】　請求項２２に記載のシステムにおいて、前記エイリアス発信元アドレスが前記実発信元アドレスより長いシステム。

【請求項２８】　請求項２２に記載のシステムにおいて、さらに、前記エイリアス発信元アドレスに基づいて入り返信メールをフィルタリングできる電子メール・フィルタを含むシステム。

【請求項２９】　電子メール（ｅ－ｍａｉｌ）メッセージを生成するシステムであって、

宛先アドレスと、

前記宛先アドレスに基づいたエイリアス発信元アドレスとを含むシステム。

【請求項３０】　請求項２９に記載のシステムにおいて、前記エイリアス発信元アドレスが前記宛先アドレスの関数であるシステム。

【請求項３１】　請求項２９に記載のシステムにおいて、前記エイリアス発信元アドレスがさらに前記電子メール・メッセージの実発信元アドレスに基づくシステム。

【請求項３２】　請求項２９に記載のシステムにおいて、前記システムが匿名リメーラとして実施されるシステム。

【請求項３３】　請求項２９に記載のシステムにおいて、前記システムが電子メール送信者のコンピュータ上で動作するシステム。

【請求項３４】　電子メール（ｅ－ｍａｉｌ）メッセージを生成する方法であって、

前記電子メール・メッセージに宛先アドレスを配置するステップと、

前記電子メール・メッセージに前記宛先アドレスに基づくエイリアス発信元アドレスを配置するステップとを含む方法。

【請求項３５】　請求項３４に記載の方法において、前記エイリアス発信元アドレスが前記宛先アドレスの関数である方法。

【請求項３６】　請求項３４に記載の方法において、前記エイリアス発信元アドレスがさらに前記電子メール・メッセージの実発信元アドレスに基づく方法。

【請求項３７】　請求項３４に記載の方法において、前記方法が匿名リメーラにおいて実行される方法。

【請求項３８】　請求項３４に記載の方法において、前記方法が電子メール送信者のコンピュータにおいて実行される方法。

【請求項３９】　電子メール（ｅ－ｍａｉｌ）メッセージであって、

宛先アドレスと、

前記宛先アドレスに基づくエイリアス発信元アドレスとを含むメッセージ。

5

【請求項４０】　請求項３９に記載のメッセージにおいて、前記エイリアス発信元アドレスが前記宛先アドレスの関数であるメッセージ。

【請求項４１】　請求項３９に記載のメッセージにおいて、前記エイリアス発信元アドレスがさらに前記電子メール・メッセージの実発信元アドレスに基づくメッセージ。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、概して、コンピュータ・ネットワークに関し、より詳細には、ネットワーク上の電子メール（「ｅ－ｍａｉｌ」）の匿名伝送と、少なくとも部分的に電子メールの宛先アドレスに基づいた入り電子メールのフィルタリングを提供するシステムおよび方法に関する。

【０００２】

【従来の技術、及び、発明が解決しようとする課題】＜関連出願への相互参照＞本出願は、本発明と共通に譲渡され、引用によって本明細書の記載に援用する「電子メールの匿名リメールとフィルタリングを提供するシステムおよび方法」と題された、１９９７年８月２８日出願の米国特許仮出願第６０／０５７，１３２号の利益を請求する。

【０００３】本発明はまた、本出願と共通に譲渡され、「ネットワークにおける匿名個人別参照を提供するシステムおよび方法」と題された、１９９７年１月２２日出願の第０８／７８７，５５７号で開示された発明に関連する。

【０００４】近年、より有効で確実かつ費用効果の高いコンピュータとネットワーキング・ツールが利用可能になったため、多くの企業および個人（集合的に「ユーザ」と呼ぶ）が絶えず発展する電子社会に参加できるようになった。コンピュータ産業全体が経験した技術の計り知れない進歩によって、こうしたユーザは、パソコン（ＰＣ）のような市販のコンピュータに依存して、自らの情報処理と通信の需要を満たすことができるようになった。このため、ＰＣ製造業者はユーザが、インターネットのようなネットワーク上の通信のために使用されるインタフェース（モデムのような）をＰＣの大部分に装備できるようにしている。インターネットは、ネットワーク（例えば、公衆および構内の音声、データ、画像およびマルチメディア・ネットワーク）の周知の集合体であり、協同して共通プロトコルを使用し、ネットワークの世界的なネットワークを形成する。

【０００５】こうした協同には、あるユーザ（「送信者」）から別のユーザ（「受信者」）への電子メール（「ｅ－ｍａｉｌ」）の通信が含まれることが多い。インターネット上で利用される従来の電子メール・プロトコルの１つである標準メール転送プロトコル（「ＳＭＴＰ」）は、各電子メール・メッセージ本文が、送信者の

6

電子メール・アドレス（「発信元アドレス」）と受信者の電子メール・アドレス（「宛先アドレス」）を含むヘッダを有することを要求している。周知の電子メール・プロトコルはすべて、受信者が送信者に電子メールを返信できるように電子メールが発信元アドレスを含むことを要求している。

【０００６】今日のコンピュータに基礎を置く社会ではプライバシーが主要な関心になっている。ユーザはコンピュータ・ネットワーク上で言葉、音声または画像で自らを表現することを望んでいるが、発信元として特定されることを望まないことがある。すなわち、ユーザは自らの真の身元を秘密にしておくことを望んでいながら、自分宛の電子メールは受信したいと考えているのである。このプライバシーの要求は、商取引から個人的思考まで、通信の広い範囲にわたっている。不都合にも、発信元アドレスを発信者の電子メールに含めるという要求によって、送信者の身元が暴露され、プライバシーを損なっている。

【０００７】この問題に対する解決法の１つがいわゆる「匿名リメーラ」である。匿名リメーラはネットワークに接続されたコンピュータ・システムで、送信者の身元を暴露せずネットワーク上で双方向電子メール通信を可能にする。送信者が電子メール・メッセージの本文中に身元情報を収納しない限り、受信者は送信者の真の身元を発見することができない。

【０００８】匿名リメールは当業技術分野で周知である。現時点でもっとも有名なインターネット・リメーラはフィンランドの“ａｎｏｎ．ｐｅｎｅｔ．ｆｉ”リメーラであったが、これはその絶頂期には５００，０００を超えるユーザを誇っていた。双方向電子メール通信をサポートするために、従来のリメーラは、実ユーザ・アドレスとエイリアス発信元アドレス（普通“ｘｘｘｘｘｘ@ｒｅｍａｉｌｅｒ．ａｄｄｒｅｓｓ”という形態を取る）を相関させる変換テーブルを維持しなければならない。匿名送信者からメッセージを受信すると、リメーラは送信者の実発信元アドレスを対応するエイリアス発信元アドレスに置換して、メッセージを目的受信者にリメールする。受信者はメッセージに返信することはできるが、それは匿名送信者のエイリアス発信元アドレスを使用することによってのみ可能である。受信者から返信を受け取ると、リメーラはエイリアス発信元アドレスの代わりに匿名送信者の実発信元アドレスを使い、匿名送信者に返信をリメールする。

【０００９】従来のリメーラの主要な問題は変換テーブル自体である。このテーブルは詳細な実発信元アドレスと、実発信元アドレスとエイリアス発信元アドレス間の相関関係を含んでいるため、ハッカーと法執行機関が共にその入手を切望している。すなわち、リメーラを保持する人物は、ハッカーから変換テーブルを保護すると共に、その人物に真の身元の保護をゆだねた送信者のプラ

7

イバシーに関する厄介な法律上の問題に直面しなければならない。

【００１０】たとえ送信者が匿名リメーラを使用することによって自分の匿名性を保護していても、彼はやはり頼んでもいない、普通コンピュータで作成された電子メール（今日のインターネットの語法では「ジャンク」電子メールまたは「スパム」と呼ぶ）の集中攻撃にさらされることがあるが、これは送信者のエイリアス発信元アドレスによって送信者と連絡を取ることができるためである。現在、こうした不必要な電子メールを防止する唯一の自動的方法は、ヘッダに含まれる発信元アドレスまたは本文に含まれる特定の語に基づいてフィルタリングすることである。不都合にも、メッセージの発信元アドレスまたは本文中の語に基づくフィルタリングはよく言っても荒削りなもので、意図せずに有効な電子メール・メッセージを削除したり、意図せずにジャンクを保存したりする危険を有している。もちろん、手動フィルタリングという選択肢もあるが、時間を犠牲にし、電子メール・メッセージに含まれる不快な内容にさらされる危険を伴っている。

【００１１】従って、当業技術分野で必要とされるものは、改善されたリメーラ、リメールの方法、および不必要な電子メール・メッセージを自動的にフィルタリングする、より有効な方法である。

【００１２】

【課題を解決するための手段】従来技術の上記で論じた欠陥を解決するために、本発明は、実発信元アドレスと宛先アドレスを有する電子メール（「ｅ－ｍａｉｌ」）メッセージのエイリアス発信元アドレスを生成するシステムおよび方法、および本システムまたは本方法を含むインターネットのようなコンピュータ・ネットワークを導入する。一実施形態では、本システムには宛先アドレスを利用してエイリアス発信元アドレスを生成するエイリアス発信元アドレス生成器が含まれる。本システムにはさらに、実発信元アドレスをエイリアス発信元アドレスで置換するエイリアス発信元アドレス置換器が含まれる。これは電子メール・メッセージから実発信元アドレスを除去し、それによって、実発信元アドレスに存在する送信者を匿名にする。本システムにはさらに、エイリアス発信元アドレス宛の電子メールを受信し、実発信元アドレスを計算し、その電子メールを実発信元アドレスに転送する電子メール転送器が含まれる。

【００１３】従って、送信者は一組のエイリアス発信元アドレスを備えているが、これは本発明のいくつかの実施形態では各宛先アドレスに固有である。しかし、本システムは自動的に発信元アドレスの生成と置換を提供するので、ユーザは多数のエイリアス発信元アドレスを追跡するタスクから開放される。

【００１４】本発明の一実施形態態では、エイリアス発信元アドレスには、他の情報と共に、実発信元アドレス

8

の暗号化バージョンが含まれる。この方法で、電子メール転送器は、エイリアス発信元アドレスがあれば、エイリアス発信元アドレスから実発信元アドレスへの変換テーブルを必要とせず、実発信元アドレスを計算することができる。この実施形態のもう１つの利点は、エイリアス生成器が電子メール転送器と連絡する必要がないことである。すなわち本システムは任意の数のエイリアス生成器と任意の数の電子メール転送器を含むことがある。エイリアス生成器と電子メール転送器はいつでもシステムに追加およびそこから除去することができる。

【００１５】本発明の一実施形態では、本システムにはさらに、エイリアス発信元アドレスに基づいて入り返信メールをフィルタリングすることができる電子メール・フィルタが含まれる。エイリアス発信元アドレスを宛先アドレスに依存させることによって、単一の送信者が一組の異なったエイリアス発信元アドレスを有することができ、送信者は希望する場合、エイリアス発信元アドレスに基づいて入り返信メールをフィルタリングすることができる。ジャンク電子メールの配布者は多くの手段によって自分の身元や望ましくないメッセージの内容を覆い隠すことができるが、電子メールをうまく送信者に送信したい場合には、配布者は送信者の正確な同じエイリアス発信元アドレスを宛名にしなければならない。従って、エイリアス発信元アドレスは、宛先アドレスとして使用される場合、ジャンク電子メールをフィルタリングし、希望する場合、ジャンク電子メール配布者がどこでそのエイリアス発信元アドレスを入手したかを判断する有効な方法をユーザに提供する。

【００１６】エイリアス発信元アドレスに基づいて電子メールをフィルタリングする能力は、エイリアス発信元アドレスを生成する個々の方法とは無関係である。この方法による電子メールのフィルタリングを可能にするためには、エイリアス発信元アドレスは宛先アドレスに依存しなければならない。エイリアス発信元アドレス生成器は、有利にも、（１）一貫性（同じエイリアスが同じ宛先に対して提示される）、（２）固有性（２つの宛先が同じエイリアスに与えられる可能性が低い）、（３）プライバシー（受信者はエイリアス発信元アドレスによって実発信元アドレスを判断できない）という３つの属性の１つかそれ以上を有する。

【００１７】本発明の一実施形態では、本システムは遠隔匿名リメーラの形態を取っており、送信者はネットワークを通じてシステムと連絡しなければならない。他の実施形態では、本システムは送信者のコンピュータ上で局所的に動作する。送信者が電子メール・メッセージを作成する際、エイリアス発信元アドレスが決定されて追加され、遠隔匿名リメーラの必要を除去する。

【００１８】以上、本発明の好適および代替的な特徴をかなり広範に概説したので、当業技術分野に熟練した者には以下の発明の詳細な説明をよりよく理解することが

できるだろう。本発明の請求項の対象を形成する本発明の付加的な特徴は以下に説明される。当業技術分野に熟練した者には、開示された概念と個々の実施形態を、本発明の同じ目的を実行する他の構成物を設計または修正する基礎として容易に使用できることを理解されたい。当業技術分野に熟練した者にはまた、こうした同等構成物がその広範な形態において本発明の精神と範囲から逸脱していないことを理解されたい。

【００１９】

【発明の実施の形態】まず図１を参照すると、本発明の原理が適切に使用され、変換テーブルなしに動作し、宛先に依存するエイリアス発信元アドレスを送信者の電子メールに割り当てる匿名リメーラを提供する分散形ネットワーク（一般に１００として示される）の例の高水準ブロック図が示される。分散形ネットワーク１００には例示としての複数のコンピュータ・システム１１０ａ、１１０ｂ、１１０ｃ、１１０ｄ、１１０ｅ、１１０ｆ、１１０ｇ、１１０ｈ、１１０ｉが含まれるが、これらは例示として互いに接続され、インターネット１１５を形成する。インターネット１１５にはワールド・ワイド・ウェブが含まれるが、これはネットワーク自体ではなく、むしろブラウザ、サーバ・サイト（複数のコンピュータ・システム１１０ａ、１１０ｂ、１１０ｃ、１１０ｄ、１１０ｅ、１１０ｆ、１１０ｇ、１１０ｈ、１１０ｉ上で動作する）、ハイパーテキスト・マークアップ言語（「ＨＴＭＬ」）ページ等の組み合わせによってもたらされる、インターネット１１５の最上部に維持される「抽象概念」である。

【００２０】例示としての実施形態はインターネット１１５のために適切に実現され、その上で使用されるが、本発明の原理と広範な範囲は、有線または無線の、何らかの適切に配置されたコンピュータ、通信、マルチメディアまたは他のネットワークに関連する。さらに、本発明の原理は、複数のコンピュータ・システム１１０ａ、１１０ｂ、１１０ｃ、１１０ｄ、１１０ｅ、１１０ｆ、１１０ｇ、１１０ｈ、１１０ｉの１つといった、単一のコンピュータ・システムを使用して示されるが、同じ範囲内の他の実施形態には１つより多いコンピュータ・システムが含まれることがある。

【００２１】例示としてのネットワーク１００には、ネットワーク１００の様々なコンピュータ・システム１１０ａ、１１０ｂ、１１０ｃ、１１０ｄ、１１０ｅ、１１０ｆ、１１０ｇ、１１０ｈ、１１０ｉの１つ１つを相互接続するよう動作する複数の（仮定上の）セキュリティのない通信チャネルが含まれるものと仮定される。通信チャネルの概念は周知であり、１つ１つの相互接続されたコンピュータ・システム間のセキュリティのない通信を可能にするものである（インターネットは、やはり周知のＳＭＴＰのような慣用の通信プロトコルを利用する）。分散形ネットワーク・オペレーティング・システムは少なくともいくつかのコンピュータ・システム１１０ａ、１１０ｂ、１１０ｃ、１１０ｄ、１１０ｅ、１１０ｆ、１１０ｇ、１１０ｈ、１１０ｉ上で動作し、それらの間の情報のセキュリティのない通信を管理する。分散形ネットワーク・オペレーティング・システムも周知である。



【００２２】図１はまた、以下の議論のために、それぞれ電子メール送信者と電子メール受信者に関連すると仮定される第１および第２ユーザのコンピュータ・システム１０５ａ、１０５ｂを示す。すなわち、送信者は自分の実発信元アドレスと、受信者に対応する宛先アドレスを個々の電子メール・メッセージに適用し、電子メール・メッセージをネットワーク１００と第２ユーザのコンピュータを通じて受信者に送信することができる。

【００２３】第１ユーザのコンピュータ・システムは特定のコンピュータ・システム１１０ａと関連させることができる（この関連は破線１２０によって示される）。この特定のコンピュータ・システム１１０ａは、第１ユーザのコンピュータ・システムのホーム・サイトおよびインターネット・サービスのプロバイダとして機能する。

【００２４】ここで図２を参照すると、一般に２００として示されるデータ処理および記憶回路のブロック図が示されるが、これは図１のネットワーク中で利用され、本発明が動作する環境を提供する。回路２００はプロセッサ２１０、揮発性記憶装置２２０、不揮発性大容量記憶ユニット２３０および通信回路２４０を含む。

【００２５】図２で例示としての回路２００の目的は広範な一連の計算プラットフォームを表すことである。従って、回路２００は、メインフレーム、ミニコンピュータまたはパソコン（「ＰＣ」）である。本発明は、何らかの特定の等級の計算プラットフォームに制限されるものではない。前に戻って図１を参照し、続いて図２を参照すると、複数のコンピュータ・システム１１０ａ、１１０ｂ、１１０ｃ、１１０ｄ、１１０ｅ、１１０ｆ、１１０ｇ、１１０ｈ、１１０ｉの各々と、第１および第２ユーザのコンピュータ・システム１０５ａ、１０５ｂは関連して図２に示される回路を有する。

【００２６】本発明は、本発明が提供するようなエイリアス発信元アドレス生成器、エイリアス発信元アドレス置換器、実発信元アドレス生成器、実発信元アドレス置換器および電子メール・フィルタを生じるようデータ処理および記憶回路２００で実行可能な一連の命令として実施される。

【００２７】ここで図３を参照すると、一般に３００として示される、実発信元アドレスと宛先アドレスを有する電子メール・メッセージのエイリアス発信元・アドレスを生成する方法の１つのきわめて特定的な実施形態の流れ図が示される。方法３００はエイリアス発信元アドレス生成器において実施される。

【００２８】この議論では、この時点で、方法３００は実発信元アドレスからエイリアス発信元アドレスを生成する方法の一例に過ぎないことが示されるべきである。本発明は特定的に列挙されるステップを要求するものではない。その代わり、本発明が要求するのは、結果として生じるエイリアス発信元アドレスが宛先アドレスに依存していることだけである。エイリアス発信元アドレス生成器は、（１）一貫性（同じエイリアスが同じ宛先に対して提示される）、（２）固有性（２つの宛先が同じエイリアスに与えられる可能性が低い）、（３）プライバシー（受信者はエイリアス発信元アドレスによって実発信元アドレスを判断できない）という３つの属性の１つかそれ以上を有するので有利である。

【００２９】本方法は開始ステップ３１０で開始されるが、ここではリメールされる電子メールが、本発明の原理によって動作するリメーラで送信者から受信される。送信者の実発信元アドレスが電子メール・メッセージから読み取られ、ステップ３２０で圧縮されて、方法３００が完了する時結果として生じるエイリアス発信元アドレスが長すぎないようにする。圧縮は、例示としての実施形態では、送信者のメールボックス名、ドメイン名および最上位ドメインで使用される文字集合に依存する可変長圧縮である。圧縮ステップは、もちろん、全く必要に応じて自由に選択されるものである。

【００３０】圧縮に続いて、方法３００はステップ３３０に進むが、ここでは周知のＭＤ５アルゴリズムによって、電子メール・メッセージの宛先アドレスのハッシュ値が計算される。宛先アドレスは宛先電子メール・アドレスのドメイン部分であるか、またはユーザに電子メール・アドレスを提供するよう要求するワールド・ワイド・ウェブ形式のユニフォーム・リソース・ロケータ（「ＵＲＬ」）のホスト部分である。ＭＤ５ハッシュ値から、２つの非並行ビット・フィールドが得られる。例示としての実施形態では、第１ビット・フィールドは２ビット長であり、第２ビット・フィールドは８ビット長である。

【００３１】圧縮と同様、ハッシュ値の計算は全く自由選択である。ステップ３３０の唯一の重要な態様は、エイリアス発信元アドレスが電子メール・メッセージの宛先アドレスに基づいてもたらされるということである。宛先アドレスの修正は（以下より些末な方法の説明で見られるように）エイリアス発信元アドレスに基づいて行われる必要はない。

【００３２】次に、ステップ３４０では、ｎ個の空白バイトが圧縮された実発信元アドレスに追加されるが、ここでｎは第１ビット・フィールドの数値に等しい。空白バイトを追加することによって実発信元・アドレスの本当の長さが隠される。また、ステップ３４０では、第２ビット・フィールドがリメーラに局所的に保存された秘密鍵に追加され、それによって宛先アドレスに固有の拡張秘密鍵が作成される。空白バイトを追加することによって実発信元アドレスの本当の長さが隠されるが、この追加は本発明の広範な範囲にとって不必要である。

【００３３】次に、ステップ３５０では、（空白バイトを追加された）圧縮された実発信元アドレスが、例えば暗号鍵として宛先アドレスに固有の拡張秘密鍵を使用するデータ暗号化規格（「ＤＥＳ」）によって暗号化される。多数のＤＥＳパスが利用され、セキュリティをさらに向上させることがある。もちろん、適用される暗号化の種類は重要ではない。暗号化はＤＥＳである必要はなく、対称形である必要もない。実際には、本発明はいかなる暗号化も必要としない。

【００３４】次に、ステップ３６０では、第２ビット・フィールドが暗号化・圧縮された実発信元アドレスに追加される。その結果はｍを基数とする変換（ｍは任意の望ましい数）を通過し、望ましい文字列が得られる。大文字と小文字の両方を含む印刷可能な英数字文字列の場合、６４を基数とする変換が使用される。小文字のみ、または大文字のみが望ましい場合、３２を基数とする変換が使用される。

【００３５】方法３００は終了ステップ３７０で終了し、エイリアス発信元アドレスの導出が完了した。すべての他のステップ３１０、３２０、３３０、３４０、３５０と同様、ステップ３６０は、望ましい結果が印刷可能な文字列からなるエイリアス発信元アドレスでないならば不必要である。エイリアス発信元アドレスは、おそらくエイリアス発信元アドレス置換器によって実発信元アドレスに置換される。

【００３６】上記で説明された例示としての方法３００を、例えば“ｆｏｏ＿ｂａｒ@ｂｅｌｌ－ｌａｂｓ．ｃｏｍ”という実発信元・アドレスと“ｗｗｗ．ｙａｈｏｏ．ｃｏｍ”という宛先アドレスを有する電子メール・メッセージに対して利用すると、発信元アドレスは“ｗｘＯｎｌｑｌＵＵＥＸＪｘｚｗＶＳｓｆＫｇＷ”に変換される。これは例示としてのリメーラのドメイン名と最上位ドメインの前に追加され、“ｗｘＯｎｌｑｌＵＵＥＸＪｘｚｗＶＳｓｆＫｇＷ@ｌｐｗａ．ｃｏｍ”という、宛先アドレス特定、ＳＭＴＰで有効なエイリアス発信元アドレスを生じる。

【００３７】上記の方法３００で示したような圧縮、ハッシュ、空白バイトの追加および暗号化が行われないより複雑でない方法を利用すると異なった結果が生じる。一例として、例えば“ｆｏｏ＿ｂａｒ@ｂｅｌｌ－ｌａｂｓ．ｃｏｍ”という実発信元・アドレスと“ｗｗｗ．ｙａｈｏｏ．ｃｏｍ”という宛先アドレスを有する電子メール・メッセージは“ｆｏｏ＿ｂａｒ．ｂｅｌｌ－ｌａｂｓ．ｃｏｍ．ｗｗｗ．ｙａｈｏｏ．ｃｏｍ”（自明な文字列の連鎖に過ぎない）に変換される。これは例示としてのリメーラのドメイン名と最上位ドメインの前に追加され、“ｗｗｗ．ｙａｈｏｏ．ｃｏｍ．ｆｏｏ＿

ｂａｒ．ｂｅｌｌ－ｌａｂｓ．ｃｏｍ@ｌｐｗａ．ｃｏｍ”を生じる。このはるかに複雑でない（かつより安全でない）方法も同様に本発明の広範な範囲内にある。方法３００で示されたステップは、このより複雑でない方法では利用されないことに留意されたい。

【００３８】上記で説明された方法３００に関する多くのことに留意されたい。第１に、秘密鍵はリメーラ・サイトに保存することが必要な唯一のデータである。残りのデータはすべて電子メール・メッセージ自体に含まれる。すなわち、従来のリメーラの変換テーブルは回避される。実際には、秘密鍵はリメーラを構成するソフトウェアにコンパイルされる。

【００３９】第２に、ワールド・ワイド・ウェブには受け入れる電子メール・アドレスの長さに何らかの制限を課しているものが多い。方法３００は実発信元アドレスより長いエイリアス発信元アドレスを生成するため、実発信元アドレスはまず圧縮され、エイリアス発信元アドレスの長さが実発信元アドレスの長さを超える度合いを小さくする。あるサイトが結果として生じたエイリアス発信元アドレスを切り捨てた場合、切り捨てられたエイリアス発信元アドレスを利用する返信メールは失われる。

【００４０】第３に、同じ実発信元アドレスに対して生成される別個の宛先アドレス特定エイリアス発信元アドレスは２からｎの累乗に制限されるが、ここでｎはステップ３３０で計算されたビット・フィールドの合計長さである。例示としての実施形態では、同じ実発信元アドレスに対して生成される宛先アドレス特定エイリアス発信元アドレスの数は１０２４である。大部分の目的にとって十分であることがわかるだろう。第２ビット・フィールドがより長ければ、エイリアス発信元アドレス空間は対応して増大する。しかし、結果として生じるエイリアス発信元アドレスは、たとえ宛先が重複しても、送信者に固有であることに特に留意されたい。

【００４１】第４に、上記で説明された方法３００は、ＤＥＳを利用するが、これは一般的に５６ビット鍵で動作する周知の秘密鍵暗号化アルゴリズムである。８ビットは第２ビット・フィールドに由来するので、秘密鍵は４８ビット長である。有効４８ビットＤＥＳより強力な暗号化が望ましい場合、多数のＤＥＳパスを使用することが可能である。

【００４２】上記で説明した方法３００のステップ３５０は、ＤＥＳの代わりに、ＩＤＥＡのような他の対称形アルゴリズム、またはＲＳＡのような非対称形暗号化アルゴリズムを利用することがある。さらに、上記で説明した方法３００のステップ３５０は、ＭＤ５の代わりにＳＨＡのような他の一方向ハッシュ関数を利用することがある。また、方法３００のステップ３１０、３２０、３３０、３４０、３５０、３６０は、セキュリティ、匿名性、速度または複雑さを劣化または向上させ、また他



の設計上の考慮事項に適宜対応するために、任意の順序で実行されること、省略されることまたは複数回実行されることがある。

【００４３】最後に、方法３００は完全に可逆的であり、エイリアス発信元アドレス（普通返信電子メールに含まれる）を、元の送信者に返信するために実発信元アドレスに変換して戻すことができることに留意されたい。これは、ｍを基数とする変換を逆変換し、第２ビット・フィールドを除去し、保存された秘密鍵と追加された第２ビット・フィールドを使用して結果として生じた文字列を解読（または多重解読）し、空白バイトを除去し、最後に以上の結果を圧縮解除して実発信元アドレスを生じることによって達成される。しかし、本発明は可逆的方法に制限されるものではなく、単方向リメールだけをサポートすることも可能であることを理解されたい。

【００４４】ここで図４を参照すると、一般に４００として示される、エイリアス発信元アドレスに基づいて不必要な電子メール・メッセージをフィルタリングし、電子メール・メッセージを実発信元アドレスに転送する方法の一実施形態の流れ図が開示される。方法４００は電子メール・フィルタにおいて実行される。電子メール・転送器の説明される実施形態は実発信元アドレス生成器と実発信元アドレス置換器からなる。

【００４５】本発明の一実施形態では、本システムにはさらに、エイリアス発信元アドレスに基づいて入り返信メールをフィルタリングできる電子メール・フィルタが含まれる。エイリアス発信元アドレスを宛先アドレスに依存させることによって、単一の送信者が異なったエイリアスを有することができるので、送信者は希望する場合、エイリアス発信元アドレスに基づいて入り返信メールをフィルタリングすることができる。ジャンク電子メールの配布者は多くの手段によって自分の身元や不必要なメッセージの内容を隠すことができるが、自分の電子メールを送信者の実発信元アドレスにうまく返信したい場合、同じエイリアス発信元アドレスを正確に使用せざるを得ないので、それによってジャンク電子メールをフィルタリングし、希望する場合、どの宛先アドレスから配布者がそのエイリアス発信元アドレスを入手したかを判断する有効な根拠が提供される。

【００４６】この時点で、用語の混乱が生じることがあるが、それは返信の場合、元の電子メール・メッセージの受信者が返信電子メール・メッセージを作成するので、受信者の方が送信者となるからである。従って、混乱を減らすために、受信者は継続して「受信者」と呼び、送信者は継続して「送信者」と呼ぶことにするが、返信電子メールは「受信者」から「送信者」に送られることを理解されたい。

【００４７】従って、方法４００は開始ステップ４１０で開始され、ステップ４２０に進むが、ここでは返信電

15

子メール・メッセージが受信者から受信される。方法４００は続いてステップ４３０に進むが、ここではエイリアス発信元アドレスが返信電子メール・メッセージから読み取られる。次に、決定ステップ４４０で、そのエイリアス発信元アドレスが、送信者によって供給された拒否すべきエイリアス発信元アドレスのリストに含まれるエイリアス発信元アドレスと比較される。

【００４８】エイリアス発信元アドレスがリストの項目の１つと一致する場合（決定ステップ４４０のＹＥＳの選択肢に進む）、その返信電子メールは削除され、送信者はそれを受信しないですむ。エイリアス発信元アドレスがリストの項目のどれとも一致しない場合（決定ステップ４４０のＮＯの選択肢に進む）、本方法は続いてステップ４５０に進むが、そこでは（おそらく上記で説明した例示としての方法３００を逆転することによってか、またはおそらくエイリアス発信元アドレスから実発信元アドレスを生成する実発信元アドレス生成器によって）実発信元アドレスが導出され、おそらく実発信元アドレス置換器によってエイリアス発信元アドレスに代わって返信電子メールに代入される。

【００４９】次に、ステップ４６０で返信電子メールは送信者に転送される。本方法は終了ステップ４７０で終了し、フィルタリング転送が達成された。

【００５０】方法３００と同様に、方法４００のステップ４１０、４２０、４３０、４４０、４５０、４６０はセキュリティ、匿名性、速度または複雑さを劣化または向上させ、また他の設計上の考慮事項に適宜対応するために、任意の順序で実行されること、省略されることまたは複数回実行されることがある。

【００５１】上記に対する代替方法では、リメーラは単に返信電子メールのエイリアス発信元アドレスをヘッダ

16

のフィールドまたは返信電子メールの本文に移動し、返信電子メールをフィルタリングなしに送信者に転送することができる。その後送信者の電子メール・クライアント・プログラムが送信者が指定した基準に基づいて電子メールをフィルタリングすることができる。

【００５２】エイリアス発信元アドレスは送信者が作成した電子メールの宛先アドレスに調節されているので、送信者はある特定のエイリアス発信元アドレス宛の入り返信電子メールをフィルタリングし、自分の他のエイリアス発信元アドレスが影響を受けていないと確信することができる。受信者は、返信電子メールが適当な送信者に届くようにしたい場合、エイリアス発信元アドレスを変更する余地はない。従って、好ましくない返信電子メールは自分の姿を偽ることはできない。

【００５３】本発明が詳細に説明されたが、当業技術分野に熟練した者は、その広範な形態において本発明の精神と範囲から逸脱することなく、さまざまな変化、置換および変更がなし得ることを理解されたい。

【図面の簡単な説明】

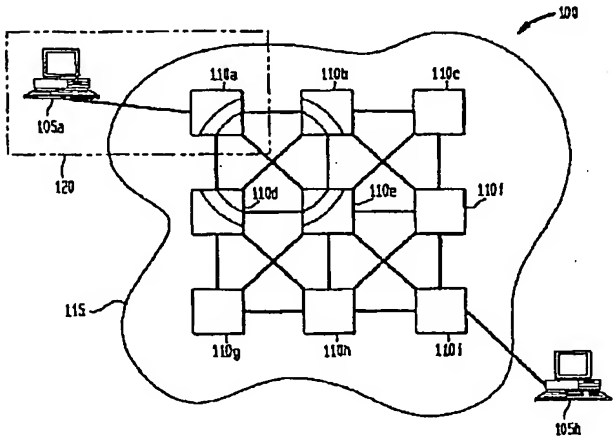
【図１】本発明の原理が適切に使用される、分散形ネットワークの例の高水準ブロック図を示す。

【図２】図１のネットワークで利用され、本発明が動作する環境を提供するコンピュータ・システムのブロック図を示す。

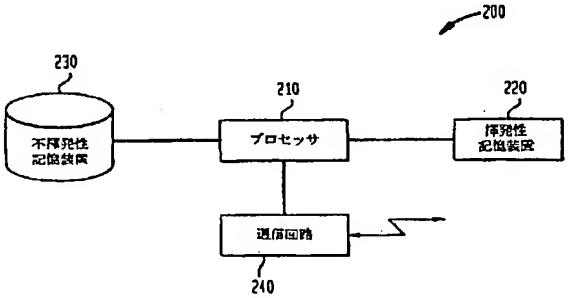
【図３】実発信元アドレスと宛先アドレスを有する電子メール・メッセージのエイリアス発信元アドレスを生成する方法の１つの特定の実施形態の流れ図を示す。

【図４】エイリアス発信元アドレスに基づいて望ましくない電子メール・メッセージをフィルタリングし、電子メールを実発信元アドレスに転送する方法の１つの特定の実施形態の流れ図を示す。

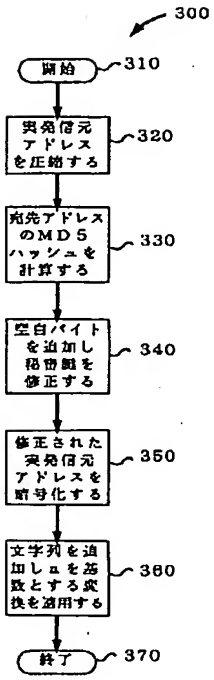
【図１】



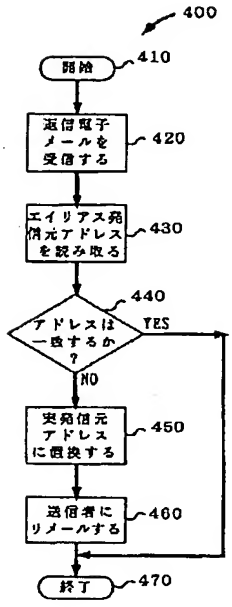

【図２】



【図３】




【図４】




---

フロントページの続き

(72)発明者　フィリップ　ビー．ギボンズ
アメリカ合衆国　07090　ニュージャーシィ，ウエストフィールド，エンブリー　コート　201
(72)発明者　ディヴィッド　モリス　クリストル
アメリカ合衆国　07901　ニュージャーシィ，サミット，リンデン　プレイス　3
(72)発明者　ヨッシ　マティアス
イスラエル国　69697　テル　アヴィヴ，ハミッシュマー　ハエツラチ　12
(72)発明者　アライン　ジュールズ　メイヤー
アメリカ合衆国　10025　ニューヨーク，ニューヨーク，アパートメント　3，ウエスト　100　ストリート　309